Australian Air League
Data Breach Response Plan

Policy number	1.19	Version	1
Drafted by	Moores	Approved by Council of AAL	5th March 2019
Responsible person	Chief Commissioner	Scheduled review date	30th December 2020

19.0 INTRODUCTION

19.1 Purpose

19.1.1 When stakeholders disclose their personal information to us, they are placing trust in Australian Air League (**the League**) to protect their personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

19.1.2 The League is required to keep personal information safe and secure in accordance with strict legal obligations and it is our expectation that al members assist the League comply with its obligations.

19.1.3 It is essential that all members (across all levels of the organisation) are proactive in responding to a data breach incident and that they take such preventative action necessary before any serious harm occurs to the affected individuals.

19.2 Scope

19.2.1 This Data Breach Response Plan (**Plan**) applies to all members and adult supporters engaged by the League and is to be applied in the event that a data breach occurs, or is suspected to have occurred, pursuant to the *Privacy Act 1988* (Cth).

19.2.2 "Member" means any person who holds a Certificate of Membership issued by the League. This includes:

a. Uniformed members under 18 years of age (Cadet Members);

b. Members 18 years of age and over (Adult Members);

c. Uniformed Adult Members; and

d. Non Uniformed Adult Members (Associate).

19.2.2 "Adult Supporter" means an adult who, from time to time, assists the League in some way (but who is not a Member).

19.3 What is a data breach?

19.3.1 Data breach means when personal information held by the League is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

19.3.2 Data breaches occur in a number of ways. Some examples include:

a. laptops, removable storage devices, or paper records containing personal information being lost or stolen;

b. databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the League;

c. paper records stolen from insecure recycling or garbage bins;

d. the League mistakenly providing personal information to the wrong person, for example by sending details to the wrong address; and

e. an individual deceiving the League into improperly releasing the personal information of another person.

19.4 Response team

19.4.1 The Response Team is comprised of the members outlined in **Schedule A**.

19.4.2 It is the responsibility of the Team Leader (or if they are not available, the Deputy Team Leader) to implement the Plan or delegate responsibilities to ensure that the Plan is implemented.

STEP 1: CONTAIN THE BREACH AND DO A PRELIMINARY ASSESSMENT

19.5 Notify the Response Team

19.5.1 Any person that suspects a data breach may have occurred, or is likely to occur, must:

a. use reasonable measures to contain the breach (if possible) as soon as practicable; and

b. make a report to the Response Team using info@airleague.com.au and marking in the subject line the words "SUSPECTED DATA BREACH" as soon as practicable and no later than 48 hours after a suspected breach has occurred.

19.5.2 Failure to comply with clause 19.5.1 may result in disciplinary action.

19.5.3 Once a report under clause 19.5.1 has been made, the Team Leader will implement immediate action to:

a. contain the breach to the extent possible (e.g. stop the unauthorised practice, recover the records, or shut down the system that was breached); *and*

b. take steps to mitigate the harm an individual may suffer as a result of a breach (as necessary).

19.6 Preliminary assessment

19.6.1 The Team Leader will as soon as practicable make enquiries, and record the enquiries in writing, in relation to the following:

a. What personal information does the breach involve?

b. What was the cause of the breach?

c. What is the extent of the breach?

d. What are the harms (to affected individuals) that could potentially be caused by the breach?

e. How can the breach be contained?

19.6.2 Once the Team Leader has carried out the enquiries in clause 19.6.1, the Team Leader will inform the Response Team about the findings.

STEP 2: EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

19.7 Risk assessment

19.7.1 The Team Leader will complete the form in **Schedule B**.

19.7.2 Relevant factors to consider to assess the risks are:

a. The type of personal information involved;

b. The context of the affected information and the breach;

c. The cause and extent of the breach;

d. The risk of serious harm to the affected individuals; and

e. The risk of other harms.

19.7.3 The Team Leader, in consultation with the Response Team, will determine whether an eligible data breach has occurred.

19.8 Eligible data breach

19.8.1 An eligible data breach happens if:

a. there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and

b. the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

19.8.2 The Team Leader is required to complete the form in **Schedule C** and use this information to make a decision as to whether an eligible data breach has occurred or not.

19.8.3 If an eligible data breach has occurred, go to clause 19.9.

STEP 3: NOTIFICATION

19.9 Notification if eligible data breach

19.9.1 Unless the exception under clause 19.9.3 applies, the Team Leader will notify:

a. the Office of the Australian Information Commissioner (**OAIC**) as soon as practicable in circumstances where there are reasonable grounds to believe that an eligible data breach has happened or if directed to do so by the OAIC; and

b. all affected individuals either:

i. directly (via email and/or post); or

ii. if impracticable to notify all affected individuals directly, publish a statement on the website.

19.9.2 The notification to the OAIC in clause 19.9.1 must include:

a. the identity and contact details of the League;

b. a description of the eligible data breach that the League has reasonable grounds to believe has happened;

c. the kind or kinds of information concerned; and

d. recommendations about the steps that individuals should take in response to the eligible data breach.

19.9.3 Where:

a. there is unauthorised access to, disclosure or loss of information but the League takes action before it results in any serious harm to the affected individual; and

b. as a result of the action a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual,

then the unauthorised access or disclosure is deemed to have never been an eligible data breach.

19.10 How to notify?

19.10.1 In general, the recommended method of notification is direct – by phone, letter, email or in person – to the affected individuals.

19.10.2 Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.

19.10.3 The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach.

19.11 Who else should be notified?

19.11.1 In addition to the affected individuals, it may also be appropriate to notify the following third parties:

a. Police;

b. Insurers;

c. Credit card companies, financial institutions or credit reporting agencies; and

d. Professional or other regulatory bodies

STEP 4: REVIEW THE INCIDENT AND TAKE ACTION TO PREVENT FUTURE BREACHES

19.12 After action review

19.12.1 The League is committed to always improving its data security processes, particularly in circumstances where a data breach occurs.

19.12.2 Following a data breach, the League will implement measures to improve its data security processes in the future, such as conducting an investigation, updating policies and procedures, and providing staff training.

Australian Air League Inc.

SCHEDULE A – RESPONSE TEAM

Name	Position	Email address
Brian Grinter	Federal Marketing & Publicity Comr./Webmaster (Team Leader)	marketing@airleague.com.au
Hanson Wong	Asst. to Federal Marketing & Publicity Comr./Webmaster (Deputy Team Leader)	marketing.asst@airleague.com.au
Ian Rickards OAM	Chief Commissioner	chiefcomr@airleague.com.au
Ray King	Federal Operations Comr	operations@airleague.com.au

Australian Air League Inc.

SCHEDULE B – EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

Consider the type of personal information involved	
Is the information personal information or sensitive information?	
Does the type of information that has been compromised create a higher risk of harm?	
Who is affected by the breach?	
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	
What parties have gained unauthorised access to the affected information?	
Have there been other breaches that could have a cumulative effect?	
How could the personal information be used?	
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	
Is there evidence of theft?	
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	
What was the source of the breach?	
Has the personal information been recovered?	

Australian Air League Inc.

What steps have already been taken to mitigate the harm?	
Is this a systemic problem or an isolated incident?	
How many individuals are affected by the breach?	
Assess the risk of harm to the affected individuals	
Who is the recipient of the information?	
What harm to individuals could result from the breach?	
Assess the risk of other harms	
Other possible harms, including to the agency or organisation that suffered the breach	

Australian Air League Inc.

SCHEDULE C – ELIGIBLE DATA BREACH

An eligible data breach happens if:

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

The determination as to what is 'serious harm' is an objective 'reasonable person' test. That is, whether a reasonable person would conclude that access to or disclosure of the personal information would be likely to result in serious harm to any of the individuals to whom the information relates. "Serious harm" is to be broadly construed and may include physical, emotional, economic and financial harm as well as reputational damage.

To determine whether a reasonable person would conclude that an access to, or disclosure of, information would be likely to would not be likely to result in serious harm to any of the individual to whom the information relates, regard must be given to the factors outlined below.

Once a report is made to the Response Team relating to a data breach, the Team Leader is required to complete this form in order to consider whether an eligible data breach has occurred or not.

Factor	Response / Relevant information considered
The kind or kinds of information	
The sensitivity of the information	
Whether the information is protected by one or more security measures	
If the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome	
The persons, or the kinds of persons, who have obtained, or who could obtain, the information	
The nature of the harm	
Any other relevant matters	

Australian Air League Inc.